ROCKDALE COUNTY PRESS RELEASE

For Immediate Release
February 17, 2020

Contact: Jeannettia Owens, Manager
Department of Public Relations
(770) 278-7058

Rockdale County Ransomware Overview

ROCKDALE COUNTY, Ga. – On February 6, Technology Services received alerts that unusual activity was present on the Rockdale County network. After a brief investigation, abnormally high CPU usage was observed on several servers and the decision was made to power down all other production servers and/or disconnect the servers from the network to minimize the impact of the suspected attack. Further investigation revealed that the attack was localized to the computers connected to the Rockdalecounty.org domain. Technology Services followed the Department of Homeland Security procedures to respond to the attacks:

- Isolate the infected computer immediately. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking networks or share drives.
- Isolate or power-off affected devices that have not yet been completely corrupted. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.
- Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware.
- Contact law enforcement immediately.
- Collect and secure partial portions of the ransomed data that might exist.
- Change all online account passwords and network passwords after removing the system from the network. Furthermore, change all system passwords once the malware is removed from the system.
- Technology Services installed additional protection/detection software on every computer in the environment.

- Additional rules/settings were added to the device protection software.

As the assessment/mitigation process was underway, the determination of the current state and availability of backups started. After forensics were gathered by state and federal law enforcement, Technology Services physically removed endpoints that were infected and restored/rebuilt servers affected.

The attack was facilitated through the use of email of which 4 examples were identified. One email had an attachment and 3 others contained links that introduced a series of scripts. There is no evidence that any financial or personal information was compromised. The ransomware version encrypted Microsoft Office related files and redirected Microsoft Windows startup processes.

Cylance Protect software has been installed on Rockdale County computers since 2018 and targeted changes to the software have been made to increase the security related to the identified malware behavior. Additionally, Cylance Optics has been added to every device to increase the visibility into individual system vulnerabilities/activity. In addition to the device level protections, Proofpoint email hardening protection and CISCO Umbrella (blocking suspicious Internet addresses) protections are on the horizon. Other cybersecurity tools have also been identified to enhance the response to questionable technology activity. No malware activity has been detected for the past 96 hours. We continue to monitor and react as any possible threat is registered.

###